IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application o

Charles P. Tresser

Serial No.: 09/578,474 Group Art Unit: 3621

Filed: May 26, 2000 Examiner: Elisca, Pierre Eddy

For: METHOD AND APPARATUS FOR COMMERCE WITH FULL ANONYMITY

Honorable Assistant Commissioner of Patents
Washington, D.C. 20231

DECLARATION UNDER 37 C.F.R. §1.131

Sir:

Comes now the Declarant, Charles P. Tresser, and states and avers the following:

(1) I am the inventor of the subject matter described the above-referenced patent application and specifically, I am the inventor of the claimed invention defined by claims 1-46 of the subject application;

(2) Prior to February 23, 2000, I had completed my invention as described and claimed in the subject application in the United States. Specifically, prior to February 23, 2000, I conceived the idea of a system, method and apparatus for conducting business electronically between a first party and a second party, such that the identity of the first party is kept from the second party. This is evidenced by the disclosure statement which is attached hereto as Exhibit A and incorporated by reference herein (note that any dates redacted from Exhibit A are prior to February 23, 2000).

(3) The contents of the disclosure statement in Exhibit A were incorporated into the specification of the present invention, upon which claims 1-46 are based. For example, the disclosure includes a discussion of a method of conducting business electronically between a first party and a second party (e.g., see Exhibit A at page 4, lines 1-4 and 21-23)

which includes providing an intermediary relationship with a third party who knows an identity of the first party but no privacy-compromising information regarding a proposed electronic business transaction between the first and second parties (e.g., see Exhibit A at page 4, line 1-23; page 7, lines 2-15), and conducting the electronic business transaction between the first and second parties through the third party such that the identity of the first party is kept from the second party (e.g., see Exhibit A at page 7, lines 11-15), wherein the second party is provided with information identifying the first party only as a transactional party in the electronic business transaction (e.g., see Exhibit A at page 7, lines 2-15), and wherein the providing an intermediary relationship by the third party includes replacing an identification data about the first party with an identifier whose linkage to the identification data is known only to the third party (e.g., see Exhibit A at page 5, line 2-page 6, line 25).

4) Attached hereto as Exhibits B-H and incorporated by reference herein are additional documents which, when combined with the disclosure statement in Exhibit A, clearly demonstrate conception of the invention prior to February 23, 2000, coupled with due diligence from just before February 23, 2000 to May 26, 2000 (the filing date of this Application). It should be noted that any dates redacted from Exhibits B-H are prior to February 23, 2000.

These Exhibits include the following:

Exhibit B: letter from Stephen C. Kaufman, Esq. to Sean McGinn, Esq. directing Mr. McGinn to prepare the subject Application;

Exhibit C: letter from Sean McGinn, Esq.. to Stephen C. Kaufman, Esq including a cost estimate for preparing the subject Application;

Exhibit D: facsimile letter from Stephen C. Kaufman, Esq. approving the cost

estimate of Sean McGinn, Esq.;

Exhibit E: e-mail letter from inventor regarding a new address;

Exhibit F: letter from Sean McGinn, Esq. to Charles P. Tresser forwarding a first draft of the subject Application;

Exhibit G: letter from Sean McGinn, Esq. to Charles P. Tresser forwarding a final draft of the subject Application; and

Exhibit H: invoice evidencing activity of Sean McGinn, Esq. regarding the subject Application.

Further Declarant sayeth naught.

09/578,474
YOR.144

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

CHARLES P. TRESSER

DATE 12/11/2003

486
PVM 600

Disclosure

Created By: Charles Tresser **Created On:** 10:59:54 AM
Last Modified By: Charles Tresser **Last Modified On:** 01:17:46 PM

PVM - 38

*** IBM Confidential ***

Required fields are marked with the asterisk (*) and must be filled in to complete the form. (2)

Summary

Status	Under Evaluation
Processing Location	YOR
Functional Area	600 Kovac-Services, Applications & Solutions
Attorney/Patent Professional	Stephen C Kaufman/Watson/IBM
IDT Team	Stephen C Kaufman/Watson/IBM
Submitted Date	
Owning Division	RES
PVT Score	To calculate a PVT score, use the 'Calculate PVT' button.
Lab	
Technology Code	
Incentive Program	

Inventors with Lotus Notes IDs

Inventors: Charles Tresser/Watson/IBM

Inventor Name > denotes primary contact	Inventor Serial	Div/Dept	Manager Serial	Manager Name
Tresser, Charles P.	1508807	22/X6MA	0267 93	Pulleyblank, William R.

Inventors without Lotus Notes IDs

IDT Selection

IDT Team:	Attorney/Patent Professional:
Stephen C Kaufman/Watson/IBM	Stephen C Kaufman/Watson/IBM

Response Due to IP&L:

Main Idea

*Title of disclosure (in English):
COMMERCE WITH FULL ANONYMITY

*Idea of disclosure:
1. Describe your invention, stating the problem solved (if appropriate), and indicating the advantages of using the invention.

In the context of regular contact between a commercial organization and a customer, where the nature of he transaction heavily depends on some

Exhibit A

collection of data associated to the customer, such as the precise contract, past information, information about the transaction being made, etc..., traditional methods forced the data to be attached to the identity of the customer (the word «forced» should be understood as «forced up to unbearable duress»: most of the invention presented here could apply without modern Information Technology, but the workload would be unbearable). With the development of Information Technology, such data were first input in a computer system for better handling and processing of the transaction. A next stage of development of Information Technology allowed to begin making heavier use of the computer, in particular for data mining, to better evaluate the risk associated to each customer, to evaluate the risk of portfolios, to perform customer segmentation for different purposes (commercial and marketing strategy, pricing, etc...), and other aspects of business intelligence and use of advanced analytics.

Using such method of business intelligence has arguably been a first serious blow to customer privacy, just because business intelligence allows company to learn more about their customers than what the customers have willingly approved.

Because business intelligence has become so precious, both for marketing and related functions, and for customer relationship management purposes, some companies have used data about their customers as an asset they would sell to other companies, another serious breach to customer privacy.

While trying to limit privacy violations, and even trying to restore fuller privacy than was ever possible before the beginning of modern

COMMERCE WITH FULL ANONYMITY - continued

Information Technology, it is desirable to achieve this goal without compromising the analytic tools which have allowed better customer understanding and hereby better pricing, otherwise, the customer would have to pay for the price of reduced commercial efficiency.

We will present this invention in the very important and particularly difficult case of the insurance industry, and more precisely for auto insurance and health insurance (which would readily adapt to the simpler case of life insurance). The concerns for privacy in business insurance are far more limited, and business insurance comes in a variety of categories which would need to be properly analyzed for relevant solutions to be offered.

2. How does the invention solve the problem or achieve an advantage,(a description of "the invention", including figures inline as appropriate)?

This invention will be presented in two parts with increasing complexity:

- the first part only concerns tentative registration, prize checking etc... (this part is possibly the stage where the customer expect higher privacy as several companies can be contacted before an insurance provider will be chosen),

1- the second part concers the further relation between the insurance and the customer: each part can be used independently of whether the other part is used.

These parts can be used independently of each other, by performing trivial modefication to what is presented here.

COMMERCE WITH FULL ANONYMITY - continued

An essential ingredient of the invention is a Third Party T which will serve as intermediary between the customer and the insurance. A customer C will establish a relationship with T which will serve for all further engagements with insurance companies.

A Fourth Party F will also be involved which delivers to C a portable device P(C) which carries the biometrics of C in such a way that C can identify him or herself as the legitimate owner of P(C) without revealing his or her identity according to the methods described in Ref1 . The non duplicability and authenticity of P(C) can for instance be guaranteed using the methods disclosed in Ref4. The device P(C) delivers a serial number S(C) at each transaction, and S(C) can be read off P(C) only in the presence of C. For more privacy, it would be better that P(C) generates numbers S(C,n), where n is an integer belonging to a big set {1,2,...,N}. Then, for each new insurance and or other partner of C, a new number n is chosen for all further transaction between the two parties. In particular, if C quits I for another company and comes back to I, it can change the n associated to I. For simplicity, we will omit the use of this number n in the sequel, as using it is a trivial amelioration of the overall protocol.

The insurance I will also chose a large set of verifiers Vj, j=1,2,... which will be medical practices for health (or life) insurance, and garages in the case of automobile insurance. Any verifier will be equipped with the apparatus needed to verify portable devices as described above, and will be connected to the Internet so that they can send information to T. The relation with T can be performed using a privacy protection mechanism, involving several other parties to avoid possible collusion, as described

COMMERCE WITH FULL ANONYMITY - continued

for instance in Ref3.

When deciding to register with insurance I, C sends to T an application A. This application can be taken off the www page of I, together with a piece of software SOFT, such as a JAVA applet, which allows to encrypt using pu1(I) where (Pr1(I),pu1(I)) is the public signature scheme of I. SOFT also allows C to compute a public signature scheme (Pr2(I,C),pu2(I,C)).

The application A has a header H where all identification data about C will be written in clear together with S(C), and a body B where all personal or vehicle data of C and pu2(I,C) will be written after encryption using pu1(I). When receiving the application, T cuts off the header an replaces it by a number N(T,C,I) which is sent to I with part B of the filled application A. I can then decrypt B and decide on the level of risk and the price if the level of risk is acceptable. These decisions D will then be communicated to I after encryption using pu2(I,C) together with N(T,C,I), and I can then send pu2(I,C)(D) to C.

If needed, before sending A to I, C will have visited one or more verifiers. C identifies him or herself to each Vj it visits using S(C), and ask Vj to send S(C) to I, together with relevant data verified by Vj such as:
- the data relevant to an automobile identified with a tag as described in Ref2 for instance,
- health data associated to C identified by S(C), which number Vj reads off P(C).

This communication to I will be performed by appending to S(C) the relevant data encrypted using pu1(I), or some other key system common to

all verifiers but possibly distinct from the key system devoted to interactions with candidate customers.
In several cases, and in particular for auto insurance, aspects of the past of C, such as driver records, possible convictions, are important elements of the risk evaluation. Either Government agencies such as the DMV accept to be equipped as private verifiers, or T will ask services of some special verifier(s) whose task will be to serve as intermediaries with the official partners and associate data encoded with pul(I) to tags such as S(C), that T would then transmit to I.

The link between T and I can make more secure by using the methods of Ref3 or by making it indirect in the following way. T will post all filled applications on a dedicated WWW page after cutting off clear identification and tagging by a number N(T,C, I) which has redundancies allowing I but no other party to recognize this number as a number emitted by I. All Insurance Companies can then check for the folders so posted and will capture those using their public key. Communication back to I can similarly be performed using such a WWW page, or using the methods described in Ref3.

Payments from I to T or vice-versa need to be documented by the paying party. This can be done by attaching a tagging number to the payment. This tag is communicated to the bank of the paying party, and accompany the transaction order to the bank of the payee. The paying bank accepts the money transfer in exchange of the tag coded using a private key of the payee's bank. Such practices, or more sophisticated ones with at least similar virtues are well known and just indicated here for the sake of

completeness.

Turning now to the case when the relation between C and I has been established, so that C is a customer of I, we need to describe how I can deal with C despite ignoring who C is. In regular operations, the infrastructure described above for first contacts type of interactions allows to get all tasks done. When submitting a claim, C will address it to T, possibly after consulting with one or more verifiers Vj as needed. After processing the claim, which is obtained by I from T by the same method the original application was obtained, I will send a payment, or request for further data, or the declination of the claim, all encrypted using pu2(I,C), to T who will then transmit it to C. Anybody versed in the art would readily understand how this can be done while the nature of what C receives remains unknown from T, while I cannot access the identity of C. The only problem not covered by what has been disclosed so far is when some refusal by C of the way I handles the claim occurs.

This will be solved in stages, depending on the severity of the refusal. In the first stage, which involves reevaluation of data, the anonymity can be preserved as identification of individuals is made using S(C) and identification of vehicles is based on tag recognition. In the second stage where the judicial system needs to be involved, the anonymity is expected to be abandoned, except in judicial systems where courts accept to hear anonymous cases presented by anonymous parties. In the latter cases, the anonymity will be preserved till the end, using S(C) and recourse to T (for instance) for the payment.

COMMERCE WITH FULL ANONYMITY - continued

As usual when using keys, it is preferable that keys be changed over time. Some businesses such as Equifax, take care of such aspect of cryptograpy-heavy transactions as a professional service.

3. If the same advantage or problem has been identified by others (inside/outside IBM), how have those others solved it and does your solution differ and why is it better?
n/a

4. If the invention is implemented in a product or prototype, include technical details, purpose, disclosure details to others and the date of that implementation.
n/a

***Critical Questions (Questions 1 - 7 must be answered)**

***Question 1**
On what date was the invention workable? : Please format the date as MM/DD/YYYY.
(Workable means ie. when you know that your design will solve the problem)

***Question 2**
Is there any planned or actual publication or disclosure of your invention to anyone outside IBM? ○ Yes ● No
If yes, Enter the name of each publication or patent and the date published below.
Publication/Patent:
Date Published or Issued:
Are you aware of any publications, products or patents that relate to this invention? ○ Yes ● No
If yes, Enter the name of each publication or patent and the date published below.
Publication/Patent:
Date Published or Issued:

***Question 3**
Has the subject matter of the invention or a product incorporating the invention been sold, used internally in manufacturing, announced for sale, or included in a proposal? ○ Yes ● No
Is a sale, use in manufacturing, product announcement, or proposal planned? ○ Yes ● No
If Yes, identify the product if known and indicate the date or planned date of sale, announcements or proposal and to whom the sale, announcement or proposal has been or will be made.
Product:
Version/Release:
Code Name:
Date:
To Whom:
If more than one, use cut and paste and append as necessary in the field provided.

***Question 4**
Was the subject matter of your invention or a product incorporating your invention used in public, e.g., outside IBM or in the presence of non-IBMers? ○ Yes ● No
If yes, give a date: Please format the date as MM/DD/YYYY

***Question 5**
Have you ever discussed your invention with others not employed at IBM? ○ Yes ● No

COMMERCE WITH FULL ANONYMITY - continued

If yes, identify individuals and date discussed. Fill in the text area with the following information: the names of the individuals, the employer, date discussed, under CDA, and CDA #.

*Question 6:
Was the invention, in any way, started or developed under a government contract or project? ○ Yes ● No ○ Not sure

If Yes, enter the contract number

*Question 7:
Was the invention made in the course of any alliance, joint development or other contract activities? ○ Yes ● No ○ Not Sure

If Yes, enter the following: Name of Alliance, Contractor or Joint Developer
Contract ID number
Relationship contact name
Relationship contact E-mail
Relationship contact phone

Question 8:
Have you submitted, or are you aware of, any related disclosure submission? ○ Yes ● No

If Yes, please provide the title and docket or disclosure number below:

Question 9:
What type of companies do you expect to compete with inventions of this type? *Check all that apply.*

- ☐ Manufacturers of enterprise servers
- ☐ Manufacturers of entry servers
- ☐ Manufacturers of workstations
- ☐ Manufacturers of PCs
- ☐ Non-computer manufacturers
- ☐ Developers of operating systems
- ☐ Developers of networking software
- ☒ Developers of application software
- ☒ Integrated solution providers
- ☒ Service providers
- ☒ Other (Please specify below)

Software companies, or the retailer

Patent Value Tool (Optional - this may be used by the inventor and attorney to assist with the evaluat

(The Patent Value tool can be used by you or the evaluation team to determine the potential licensing value of your invention.)

The **Patent Value Tool** has not yet been used to calculate a score.

Post Disclosure Text & Drawings

(Form Revised